REMARKS/ARGUMENTS

Claims 1-33 are pending in the present application, of which claims 1 and 18 are independent. Claims 1-15 and 18-30 are hereby amended. Claims 16-17 and 31-33 are hereby canceled without prejudice or disclaimer of their subject matter. No new matter has been added.

OBJECTION TO THE ABSTRACT

On page 3, the Office Action objects to the Abstract. Specifically, the Examiner alleges that the Abstract "is less than the minimum 50 word limit, not in narrative form, and not much descriptive [sic]." Accordingly, Applicant hereby amends the Abstract, as shown in the attached Appendix. Therefore, Applicant respectfully requests withdrawal of the objection to the Abstract.

OBJECTION TO THE TITLE

On page 3, the Office Action objects to the Title. In response, Applicant hereby adopts the Title suggested by the Examiner, "Reduction Calculations in Elliptic Curve Cryptography." Therefore, Applicant respectfully requests withdrawal of the objection to the Title.

OBJECTIONS TO THE SPECIFICATION

On page 3, the Office Action objects to the arrangement of the specification. With respect to the disclosure objection, Applicants respectfully decline to add section headings because the indicated suggestions in 37 C.F.R. § 1.77(b) are not statutorily required for filing a non-provisional patent application under 35 U.S.C. § 111(a). As set forth in 37 C.F.R. § 1.51(d), the suggested headings are only guidelines that are suggested for Applicant's use. Thus, Applicant respectfully submits that the section heading are not mandatory.

Moreover, Applicant notes that when 37 C.F.R. § 1.77(b) was amended in 1996 (61 FR 42790, Aug. 19, 1996), Bruce A. Lehman, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks, stated in the Official Gazette: "Section 1.77 is permissive rather than mandatory . . . . 1.77 merely expresses the Office's preference for the arrangement of the application elements. The Office may advise an applicant that the application does not comply with the format set forth in 1.77, and suggest this format for the applicant's consideration; however, the Office will not require any application to comply with the format set forth in 1.77."

Accordingly, Applicants respectfully decline to amend the specification to include the suggested section headings, and respectfully request that this objection to the specification be withdrawn.

On page 4, the Office Action alleges that important variables "should be carefully defined as to provide a clear understanding of the claimed invention." While the Examiner indicates that appropriate correction is required, the Examiner provides no information regarding the nature of such a correction. In particular, Applicant is mindful of the prohibition on adding new matter to the specification and requests clarification regarding what sort of correction would be acceptable to the Examiner. Therefore, Applicant respectfully requests withdrawal of this objection to the specification. Should the Examiner persist in objecting to the "important variables," Applicant respectfully requests a detailed explanation of how they are to be "carefully defined" to satisfy the Examiner's request.

OBJECTIONS TO THE CLAIMS

On page 4, the Office Action objects to claim 1. In response, Applicant amends claim 1 to correct the spelling error identified by the Examiner. Therefore, Applicant respectfully requests withdrawal of the objection to claim 1.

On page 5, the Office Action objects to claims 1, 5, 18, and 22. In response, Applicant deletes the subject matter identified by the Examiner, "multiple of a modulus," from claims 1, 5, 18, and 22. Therefore, Applicant respectfully requests withdrawal of the objection to claims 1, 5, 18, and 22.

On page 5, the Office Action objects to claim 13. In response, Applicant amends claim 13 to correct the spelling error identified by the Examiner. Therefore, Applicant respectfully requests withdrawal of the objection to claim 13.

On page 5, the Office Action objects to claim 17. In response, Applicant hereby cancels claim 17. Therefore, Applicant respectfully requests withdrawal of the objection to claim 17.

On page 5, the Office Action objects to claim 22. In response, Applicant amends claim 22 to delete the subject matter identified by the Examiner, "(10-17)." Therefore, Applicant respectfully requests withdrawal of the objection to claim 22.

On page 5, the Office Action objects to claim 27. In response, Applicant amends claim 27 to correct the capitalization error identified by the Examiner. Therefore, Applicant respectfully requests withdrawal of the objection to claim 27.

On page 5, the Office Action objects to claim 28. In response, Applicant amends claim 28 to correct the spelling error identified by the Examiner. Therefore, Applicant respectfully requests withdrawal of the objection to claim 28.

REJECTIONS UNDER 35 U.S.C. § 112

On page 5, the Office Action rejects claims 1 and 18 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "the number" on line 4 of both claims.

In response, Applicant hereby replaces the definite article "the" with the indefinite article "a" in the cited location. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 6, the Office Action rejects claims 6 and 23 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "the last multiplication" and "the selected number." In response, Applicant hereby replaces the definite article "the" with the indefinite article "a" in the cited locations. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 6, the Office Action rejects claims 7 and 24 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "n_0." In response, Applicant adds "the first variable" before "n_0." Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 6, the Office Action rejects claims 8 and 25 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "the carry c" and "the addend." In response, Applicant hereby replaces the definite article "the" with the indefinite article "a" in the cited locations. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 6, the Office Action rejects claims 9 and 26 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "the number." In response, Applicant hereby replaces the definite article "the" with the indefinite article "a" in the cited location. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 6, the Office Action rejects claims 9-10 and 26-27 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "k-2." In response, Applicant respectfully traverses this rejection because articles are normally not used with mathematical variables. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 6, the Office Action rejects claims 10 and 27 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "the next calculation" and "the number." In response, Applicant hereby replaces the definite article "the" with the indefinite article "a" in the cited locations. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 7, the Office Action rejects claim 21 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that there is insufficient antecedent basis for "the combined multiplication operations and

reduction operation." In response, Applicant respectfully traverses this rejection because claim 20 provides a proper antecedent for this subject matter. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 7, the Office Action rejects claim 30 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that the subject matter of this claim is unclear due to the use of "81." In response, Applicant deletes "81" in the locations described by the examiner. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 7, the Office Action rejects claim 31 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In response, Applicant hereby cancels claim 31. Therefore, Applicant respectfully requests withdrawal of this rejection.

On page 7, the Office Action rejects claim 32 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In response, Applicant hereby cancels claim 32. Therefore, Applicant respectfully requests withdrawal of this rejection.

On pages 7-8, the Office Action rejects claim 33 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In response, Applicant hereby cancels claim 33. Therefore, Applicant respectfully requests withdrawal of this rejection.

REJECTION UNDER 35 U.S.C. § 101

On page 8, the Office Action rejects claims 1-33 under 35 U.S.C. § 101 for allegedly failing to recite statutory subject matter. Applicant respectfully traverses this rejection for the reasons listed below.

Independent method claim 1 now recites, in part, the following subject matter: "A method of performing a reduction operation in a cryptographic calculation in a **digital computer**" (emphasis added). Similar subject matter now appears in independent apparatus claim 18. Applicant respectfully submits that recitation of a digital computer qualifies as statutory subject matter because a digital computer is a particular machine. Therefore, independent claims 1 and 18 now recite statutory subject matter.

Claims 2-15 depend from independent claim 1. Claims 19-30 depend from independent claim 18. Thus, Applicant respectfully submits that claims 2-15 and 19-30 also recite statutory subject matter. Claims 16-17 and 31-33 have been canceled. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1-33 under 35 U.S.C. § 101.

REJECTION UNDER 35 U.S.C. § 102

On pages 13-17, the Office Action rejects claims 1-5, 14-22, and 31-33 under 35 U.S.C. § 102(b) as allegedly anticipated by U.S. Patent No. 6,366,673 to

Hollmann et al. (hereinafter "Hollmann"). Applicant respectfully traverses this rejection for the reasons listed below.

Independent method claim 1 now recites, in part, the following subject matter: "multiplying a **first variable n_0'** by a **second variable r_3** to produce a first result; adding the first result to a **third variable r_1** and a **fourth variable Br_2** to produce a first sum; dividing the first sum into an upper half and a lower half; multiplying the upper half by the first variable n_0' to produce a second result; adding the second result to the lower half and a **fifth variable r_0** to produce a second sum; thereby permitting use of the second sum as the modulus" (emphasis added). This subject matter finds support in the specification, for example, in paragraphs [077-0083] and is depicted in Figure 3. Similar subject matter appears in independent claim 18.

Independent apparatus claim 18 further recites, in part, the following subject matter: "a plurality of input registers that store a plurality of input operands; a plurality of output registers that store a plurality of outputs; and a **multiplier** that produces said outputs using a function that operates on variables from both said input registers and said output registers" (emphasis added). This subject matter finds support in the specification, for example, in paragraphs [0097-0104] and is depicted in Figure 5.

Applicant respectfully submits that Hollmann does not disclose, suggest, or teach this subject matter. Specifically, while Hollmann does disclose modular exponentiation, Hollman clearly lacks the recited combination of multiplying a **first variable n_0** by a **second variable r_3** to produce a first result. Applicant respectfully submits that Hollman also lacks adding the first result to a **third variable r_1** and a **fourth variable Br_2** to produce a first sum. Applicant further submits that Hollman lacks dividing the first sum into an upper half and a lower half; multiplying the upper half by the first variable n_0 to produce a second result; and then adding the second result to the lower half and a **fifth variable r_0** to produce a second sum; thereby permitting use of the second sum as the modulus. Thus, Applicant respectfully submits that independent claims 1 and 18 are allowable over Hollmann.

Claims 2-5 and 14-15 depend from independent claim 1. Claims 19-22 depend from independent claim 18. Thus, Applicant respectfully submits that claims 2-5, 14-15, and 19-22 are allowable at least on the basis of their respective dependencies from allowable independent claims. Claims 16-17 and 31-33 are hereby canceled. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1-5, 14-22, and 31-33 under 35 U.S.C. § 102(b).

REJECTIONS UNDER 35 U.S.C. § 103

On pages 17-19, the Office Action rejects claims 6, 7, 23, and 24 under 35 U.S.C. § 103(a) as allegedly unpatentable over Hollmann in view of Published U.S. Patent Application No. 2002/0010730 to Blaker (hereinafter "Blaker"). On pages 19-23, the Office Action rejects claims 8, 9, and 25-27 under 35 U.S.C. § 103(a) as allegedly unpatentable over Hollmann in view of U.S. Patent No. 6,240,436 to McGregor (hereinafter "McGregor"). On page 23, the Office Action rejects claim 10 under 35 U.S.C. § 103(a) as allegedly unpatentable over Hollmann in view of Blaker, and further in view of McGregor. On page 24-29, the Office Action rejects claims 11-13 and 28-30 under 35 U.S.C. § 103(a) as allegedly unpatentable over Hollmann in view of the article to Lenstra et al (hereinafter "Lenstra"). Applicant respectfully traverses this rejection for the reasons listed below.

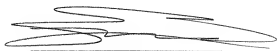
Applicant respectfully submits that Blaker, McGregor, and Lenstra fail to remedy the deficiencies of Hollman described above for independent claims 1 and 18. Claims 6-13 depend from independent claim 1. Claims 23-30 depend from independent claim 18. Thus, Applicant respectfully submits that claims 6-13 and 23-30 are allowable at least on the basis of their respective dependencies from allowable independent claims. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 6-13 and 23-30 under 35 U.S.C. § 103(a).

CONCLUSION

In view of the remarks above, Applicant believes that each of the rejections/objections has been overcome and the application is in condition for allowance. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, Aaron Waxler, of NXP Corporation at (914) 860-4296.

In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account.

Respectfully submitted,
KRAMER & AMADO, P.C.



Date: February 17, 2009

Arlir M. Amado
Registration No.: 51,399

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131
CUSTOMER NO.: 65913